aria CYBERSECURITY SOLUTIONS

Case Study – Large Muti-site Manufacturer

How a Large Manufacturer Boosted Its Protection Against a New Wave of Cyberattack

Current Cybersecurity Solutions Are Leaving Production Lines Vulnerable to Attack and Disruption – Here's How One Firm Addressed the Problem

Overview – In this case study, we will examine the cybersecurity challenges/requirements faced by a multi-site manufacturer and how the deployment of ARIA AZT PROTECT™ addressed them. The challenges/requirements stated here, provided by a specific manufacturer, are universally applicable to general cases of mid-sized to large manufacturers, defined as having independently run plants.

Keeping production lines running is the lifeblood of any manufacturing company. Disruption and unplanned downtime negatively impact the bottom line, potentially leading to millions of dollars in revenue loss. Unlike in the IT environment, operational technology (OT) that controls critical production lines is expected to run for prolonged periods – often for several months – without shut-down maintenance windows. Devices are not allowed access to the Internet for continuous updating. Furthermore, OT devices are often in place for the entire lifespan of the production line, running on legacy operating systems that can be decades old, thus allowing the manufacturer to sustain profitability as well as production targets.

Prior Mode of Operation: Production Protection – The manufacturer's prior mode of operation (PMO) included the following protections of their OT infrastructure. It focuses on creating limited access to where critical production applications run and are therefore most vulnerable: HMI (Human Machine Interface) devices, EWS (Engineering Work Stations) and data historians.

- Use of passive network security focused on limiting corporate and Internet access to (and from) the manufacturing floor to make it less accessible to attacks.
- Legacy signature-based AV systems – challenged by limiting updates to annual maintenance windows and their lack of ability to stop modern polymorphic malware, which gets past signature detection.
- Vendors and contract services providers use the internet to get access during scheduled maintenance windows via VPN.
- Vendors and contract services also are asked to use AV-protected maintenance laptops to provide device application updates and troubleshooting during these windows.
- There is limited staff (typically one person) full or part time at a plant responsible for keeping the devices and applications working, providing asset management, reporting, and overseeing data security. In many cases, this person is responsible for multiple regional plants.
- Staff have limited time to learn and operate advanced security measures. There is no time to continuously monitor and fine-tune cybersecurity tools.

Challenges/Requirements presented to ARIA – As attacks on critical infrastructure, including manufacturing, continue to rise so do the requirements for improved protection from these attacks. This is further complicated by the operational characteristics of OT environments as noted above.

The PMO did not meet the organization's requirements to protect it from increasingly sophisticated attacks, including those that get through via the supply chain. The following new requirements were identified:

- HMIs, EWS, Historians, and other devices require their OS platform and applications to be protected from all forms of ransomware/malware, supply-chain attacks, and sophisticated breach (APT) attacks, under the following constraints:
    - Replace legacy ineffective signature based Anti Virus agents which don't detect today's Malware
    - Must do so without Internet-connected AV or IOC updates and/or application patches.
    - Must be able to work fully air-gapped for up to a year and retain efficacy of protection.
    - Must stop all attacks automatically without human involvement, before production is impacted.
    - Must be able to lock down certain devices so that no unapproved application nor existing application updates will run until approved.
    - Must run on a variety of platforms, from current Windows server/ Windows desktop OS, back to Windows XP SP2.
    - Must provide reports to help ensure insurance policy and SEC rule compliance.
- Environment related.
    - Must deploy factory-wide, coming up fully protected within a four-hour window for all site devices.
    - Must be a simple to deploy and operate solution with no need for formal training due to limited time for onboarding.
    - IT wants the solution to automatically export the appropriate reports for compliance purposes, as well as securely send forensic syslog information formatted for the IT organization's SIEM.

Considered Solutions

A number of solutions were analyzed for thier ability to meet the requirements including:

Application Allow Listing Solutions

- While these solutions lock down systems to assure only approved applications run, they only run at the time the OS or the applications are started or restarted. They do not provide protection from attacks to the approved applications while they are running.
- To counter this, the vendor recommended continuous patching to mitigate application vulnerabilities. However, this technique requires rebooting the production environment continuously.
- Application Allow Listing did not stop fileless malware nor sophisticated attacks by the contracted Red Team.

- These solutions proved difficult to run out-of-the-gate and had to be tuned by skilled, trained staff to allow the applications to continue to run with every patch update, or when rarely run applications were activated for the first time.

Next Generation AV

The IT side of the organization used the industry's leading next-generation anti-virus (NGAV) and endpoint detection and response (EDR) solutions, and proposed these solutions be deployed.

- These solutions do not rely on signatures but known patterns of attacks (IOCs) that have been seen before in other customer environments.
- The challenge for the OT organization was that the solution required the OT devices to be continuously connected to the internet for monitoring and to receive updates from the vendor's cloud.
- Updates could be queued and tested on lab devices but could not be loaded to production devices until the annual maintenance window – negating their value.
- The solution did not run on the older windows OS, which would leave critical devices unprotected.
- The Red Team was able to use standard techniques to bypass the protections – similar to those used in the SolarWinds and other supply chain attacks.
- The vendor also recommended continuous patching to mitigate application vulnerabilities – however this technique also required rebooting the production environment continuously and was rejected.

ARIA AZT PROTECT

This solution uses a different approach. Similar to application allow listing, it can lock down applications and the OS preventing anything unapproved from running, including malware and ransomware. However, it goes beyond these solutions by continuously monitoring how the applications execute in memory, to provide continuous protection from any form of attempted adulteration to the running applications. In addition, it provides additional measures that stop the common techniques used by sophisticated attacks, including misuse of OS processes, shellcode, injections, and privilege escalations. The combination was intended to stop sophisticated attacks such as those coming in via supply chains that commonly have access into OT environments.

Results

- The solution was able to learn the applications on the device and prevent new unapproved applications from running – out of the box.
- The solution blocked all ransomware and malware, including fileless malware attacks launched by the Red Team
- The solution prevented code adulteration attacks on the applications with unpatched vulnerabilities, while running.
- The solution successfully defended against the Red Team attempts to misuse OS processes, shellcode, injections, and privilege escalations as seen in sophisticated supply-chain attacks.

- The solution ran successfully defending all attacks while being fully air gapped.
- The solution did not need updates to stop new attacks.
- The solution supported all legacy operating systems and did not negatively impact production application performance.
- The solution provided the reporting required for SEC and other compliance in addition to exporting syslog formatted alert data into IT's SIEM for further analysis.

Additional benefits:

- The solution provided a complete inventory of all applications and versions running and their status on each device and in each device group.
- The solution was able to block code level application exploits of unpatched vulnerabilities. This solves the problem of waiting months to receive patches from vendors once a CVE is published. This means security patches could be safely delayed until maintenance windows.
- The solution was generic enough to stop unknown vulnerabilities – such as the Pool Party novel process thread attacks discovered in December of 2023. In this case, AZT code that had been deployed six months prior stopped all eight attacks with no updates required. The IT endpoint solution completely missed stopping these attacks.
- Provided forensic alert data useful to benchmark the safety at each site and line.
- The solution was able to be loaded on running devices without reboot.
- The solution was easy for OT staff to deploy and successfully operate with minimal training.

Summary – ARIA's AZT PROTECT solution was selected because it met and exceeded the requirements, while other market leading solutions fell short.

AZT PROTECT is a proven solution designed to protect against the most dangerous new forms of cyberattack. AZT PROTECT is being deployed in industrial settings that use OT to manage production infrastructure supporting functions such as manufacturing, energy, utilities, and distribution.

Learn more or schedule an ARIA AZT demo at - https://www.ariacybersecurity.com/aria-azt-protect/

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. ARIA's solutions provide new ways for organizations to protect their most critical assets—they can shield their critical applications from attack with our AZT solution, while monitoring internal traffic, device-level logs, and alert output with our ARIA ADR solution to substantially improve threat detection and surgically disrupt cyberattacks and data exfiltration. Rounding out the portfolio, Aria's AZT Gateway Software allows us to interrogate network packets at 100mbps line-rate to enforce forwarding and capture policies on the fly. Customers in a range of industries rely on our solutions to accelerate incident response, automate breach detection, and protect their most critical assets and applications—no matter where they are stored, used, or accessed.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854
Connect with Us: info.ariacybersecurity.com/azt-demo • ARIAsales@ariacybersecurity.com • 800.325.3110
Follow Us: Linkedin